3Н

УДК 004. 415.24, 519.22;

Л.Л. Никитенко
Институт кибернетики им. В.М. Глушкова НАН Украины, г. Киев, Украина
Украина, 0368, пр. Академика Глушкова, 40

Методы стеганоанализа на основе технологии калибровки программ

L.L. Nikitenko
Institute of Cybernetics Glushkov National Academy of Sciences of Ukraine, Kiev, Ukraine
Ukraine, 0368, etc. 40 Glushkov

Methods Based on Steganalysis Calibration Technology Programs

Л.Л. Нікітенко
Інститут кібернетики ім. В.М. Глушкова НАН України, м. Київ, Україна
Україна, 0368, пр. Академіка Глушкова, 40

Методи стеганоаналізу на основі технології калібрування гістограм

Работа посвящена обзору методов статистического стеганоанализа цифровых изображений, созданных на основе оценки центра масс дискретного преобразования Фурье гистограммы изображения. Теоретические основы для создания технологии рассматриваемых методов разработаны в предположении об аддитивном встраивании дополнительной информации. Влияние аддитивного искажения на статистику сигнала исследовалось для нормы встраивания $\alpha \le 100\%$. Рассмотрены детекторы обнаружения встроенной информации, требующие проведения процедуры выбора порога обнаружения, и детекторы с использованием оценки гистограммы гипотетического сглаженного изображения.
Ключевые слова: стеганоанализ, гистограмма гипотетического сглаженного изображения, аддитивное встраивание.

Work is devoted the review of statistical steganoanaliz methods of digital images, that created on the basis of estimation of centre-of-mass of discrete Fourier transformation of image histograms. Theoretical bases for creation of technology of the examined methods are developed in supposition about additive hiding of additional information. Effect of additive distortion on signal statistics was analyzed for the hiding norm $\alpha \le 100\%$. Embedded information detectors are considered that requiring selection procedure of detection threshold and that using the histogram of a hypothetical smoothed image.
Key words: steganalysis, the histogram of a hypothetical smoothed image, additive embedding.

Робота присвячена огляду методів статистичного стеганоаналізу цифрових зображень, що базуються на оцінці центру мас дискретного перетворення Фур'є гістограми зображення. Теоретичні основи для створення технології, розроблені за умови адитивного вкраплення додаткової інформації. Досліджувався вплив адитивного вкраплення на статистику сигналу, коли норма вкраплення $\alpha \le 100\%$. Розглядалися детектори виявлення вкрапленої інформації, що потребують процедури визначення порогу виявлення, та детектори з використанням оцінки гістограми гіпотетичного згладженого зображення.
Ключові слова: стеганоаналіз, гістограма гіпотетичного згладжуваного зображення, адитивне встраювання.

Введение

Одним из новых направлений статистического стеганоанализа является создание детекторов обнаружения встроенной информации с использованием дискретного преобразования Фурье гистограммы цифровых изображений. Работа посвящена обзору зарубежных научных публикаций, касающихся технологии для создания таких детекторов, принципов их работы и описания экспериментальных результатов [1-3].

Изначально технология для создания таких детекторов разрабатывались для стеганоанализа цифровых графичных стеганограмм, созданных методами замены наименьших значащих битов (НЗБ) [1]. Позже эта технология была использована для создания детекторов, которые использовались для различения пустых контейнеров и стеганограмм, созданных методом соответствия (matching LSB) [2]. В этом методе нет четкой асимметрии как в методе замены НЗБ, когда пиксель с четной величиной может только увеличиться на 1, но никогда не уменьшается, а с нечетной наоборот. Если НЗБ пикселя не совпадает с битом сообщения, в методе соответствия при встраивании бита сообщения из величины пикселя вычитается 1, или к величине пикселя добавляется 1 по некоему заданному правилу или тайному ключу. Под величиной пикселя понимается число, поставленное ему в соответствие, например яркость или цвет. Особый интерес вызывает тот факт, что в рассмотренных работах встраивание методами НЗБ могло быть выполнено не во все НЗБ пикселей изображения, пригодных для встраивания, а только в некоторую их часть α (т.е. норма встраивания α могла быть меньше единицы). Созданные по этой технологии детекторы могут успешно применяться к методам типа OutGuess [4], которые на сегодняшний день считаются наиболее стойкими к методам статистического пассивного стеганоанализа.

1 Теоретические основы для создания технологии

Теоретические основы для создания технологии были разработаны Хармзеном и Пеарлменом в работе [1]. Они первыми предложили сравнивать взвешенную нормированную оценку дискретного преобразования Фурье (ДПФ) гистограммы принятых изображений с наперед выбранным порогом. Авторы изучали влияние аддитивного искажения на статистику сигнала.

Путем моделирования процесса аддитивного встраивания сообщения, рассматривали возникающее искажение как стегошум и исследовали возможность обнаружения встроенной информации.

Пусть $h_c[n]$ – гистограмма контейнера, $h_S[n]$ – гистограмма стеганограммы, $f_\Delta[n]$ – функция распределения масс (ФРМ) встроенного сообщения. По определению ФРМ для аддитивного стегошума есть вероятность того, что значение пикселя будет изменено на n

$$f_\Delta[n] \overset{\Delta}{=} p(x_S - x_C = n), \qquad (1)$$

где x_c– значение пикселя до встраивания, x_s – значение пикселя после встраивания.

Преобразование плотности вероятности в функцию распределения масс с учетом дискретности цифрового сигнала определяется как

$$f_\Delta[n] = \int_{n-0,5}^{n+0,5} f_\Delta(x)dx.$$

Поскольку относительная частота события является состоятельной оценкой его вероятности, гистограмму $h[n]$ рассматривается как вероятность появления пикселя с заданной величиной, умноженную на число пикселей в изображении. Это позволило сформулировать и доказать теорему о свертке гистограмм.

Теорема 1 [1]. Если аддитивный стегошум в стегосистеме не зависит от контейнера, гистограмма стеганограммы равна свертке ФРМ для аддитивного стегошума с гистограммой контейнера

$$h_S[n] = h_C[n] * f_\Delta[n]. \quad (2)$$

Из теоремы 1 следует, что знание любой схемы встраивания в форме $f_\Delta[n]$ и знание $h_C[n]$ делает известной гистограмму стеганограммы.

Большинство естественных корреляций и корреляций, которые вводятся записывающими приборами, хорошо заметны в частотной области. Поэтому далее анализ встраивания авторы [1] проводили в частотной области, применяя дискретное преобразование Фурье (ДПФ)

$$X[k] = \sum_{n=0}^{N-1} x[n] e^{-\frac{2\pi jnk}{N}},$$

где N равно наибольшему значению интенсивности в изображении. Например, для полутонового 8-и битового изображения N равно 2^8 или 256. По определению характеристическими функциями гистограммы (ХФГ) называется ДПФ от ФРМ

$$\begin{aligned} F_\Delta[k] &\stackrel{\Delta}{=} DFT(f_\Delta[n]), \\ H_c[k] &\stackrel{\Delta}{=} DFT(h_c[n]), \\ H_s[k] &\stackrel{\Delta}{=} DFT(h_s[n]). \end{aligned} \quad (3)$$

ХФГ является перепредставлением гистограммы изображения в частотной области. Свертка (2) в частотной области принимает вид

$$H_S[k] = F_\Delta[k] H_C[n]. \quad (4)$$

Из (4) становится понятным, как встраивание сообщения влияет на ХФГ.

На практике для увеличения стойкости встраивания часто уменьшается норма встраивания. Пусть случайным образом из всего изображения для встраивания выбирается α-часть пикселей. Для этого случая в [1] доказана теорема 2.

Теорема 2. Пусть стегошум не зависит от контейнера и для встраивания случайным образом выбрана α-часть пикселей. Тогда гистограмма стеганограммы задается соотношением

$$h_\alpha[n] = \alpha(h_C[n] * f_\Delta[n]) + (1-\alpha) h_C[n]. \quad (5)$$

Соответственно, в частотной области равенство (5) имеет вид

$$H_\alpha[k] = \alpha(H_C[k] F_\Delta[k]) + (1-\alpha) H_c[k]. \quad (6)$$

Согласно теореме 3 [1] сложение контейнера и стегошума с битовой нормой α можно представить единой сверткой.

Теорема 3. Пусть стегошум не зависит от контейнера, и для встраивания случайно выбрана α-часть пикселей. Тогда гистограмма стеганограммы задается равенством

$$h_\alpha[n] = f^\alpha{}_\Delta[n] * h_C[n], \text{ где } f^\alpha{}_\Delta[n] \stackrel{\Delta}{=} \alpha f_\Delta[n] + (1-\alpha)\delta[n]. \quad (7)$$

Теоремы 1 – 3 позволяют однозначно определять гистограмму стеганограммы по норме встраивания α, схеме встраивания в форме $f_{\Delta}[n]$ и гистограмме контейнера $h_C[n]$.

Для создания детектора авторам [1] была нужна такая функция от гистограммы принятого изображения, значения которой должно было соответствовать общей информации о распределении энергии в гистограмме. Центр масс ХФГ (ЦМ ХФГ)

$$C(H[k]) \overset{\Delta}{=} \frac{\sum_{k\in K} k|H(k)|}{\sum_{k\in K}|H(i)|}\ , \tag{8}$$

где $k=\{0,...,(N/2)-1\}$ и N длина ХФГ, несет общую информацию о распределении энергии в ХФГ. Для ЦМ ХФГ стеганографичных систем с аддитивным шумом была доказана теорема 4. Эта теорема дает возможность разделять контейнеры и стеганограммы по значениям ЦМ ХФГ. Поэтому в качестве меры распределения энергии в ХФГ был выбран ЦМ ХФГ, определяемый по формуле (8).

Теорема 4. Если в схеме встраивания $|F_{\Delta}[k]|$ невозрастающая функция, то после встраивания ЦМ ХФГ уменьшается или остается тем же самым

$$C(H_S[k]) \le C(H_C[k]),\ k=\{0,...,(N/2)-1\}, \tag{9}$$

с равенством тогда и только тогда, когда $|F_{\Delta}[k]|=1, \quad \forall k=0,...,(N/2)-1$.

Существует множество распределений, имеющих монотонно убывающую по величине характеристическую функцию, включая Гауссиан и Лапласиан.

В работе [1] было показано, что такие стеганографические методы, как НЗБ стеганография[1], стеганография расширением спектра и аддитивная стеганография[2] на основе ДКП позволяют применять предложенную теорию и теорему 4.

Рассматриваемая теория легко расширяется для цветных RGB изображений. Рассмотрим пиксель $\vec{x}(n_1,n_2)$ как вектор интенсивностей RGB:

$$\vec{x}(n_1,n_2) = [x_r(n_1,n_2)\ x_g(n_1,n_2)\ x_b(n_1,n_2)].$$

Определим гистограмму $h[\vec{n}]$ для RGB, где $\vec{n}$ – вектор интенсивностей RGB, а величина гистограммы есть число пикселей с триплетом значений RGB. Применяя 3-мерное дискретное преобразование Фурье к $h[\vec{n}]$ получаем характеристическую функцию гистограммы ХФГ для RGB-изображения

$$H[\vec{k}] \overset{\Delta}{=} DFT_3 h[\vec{n}]. \tag{10}$$

Поскольку ДПФ симметрично относительно $N/2$, достаточно рассматривать только $[0,...,(N/2)-1]^3$ из $[0,...,N-1]^3$ коэффициентов ДПФ. Центр масс для $H[\vec{k}]$ вдоль каждой из трех осей определяется как

$$C_{k1}(H[\vec{k}]) \overset{\Delta}{=} \sum_{k\in K} k_1\left|H[\vec{k}]\right|,\ C_{k2}(H[\vec{k}]) \overset{\Delta}{=} \sum_{k\in K} k_2\left|H[\vec{k}]\right|,\ C_{k3}(H[\vec{k}]) \overset{\Delta}{=} \sum_{k\in K} k_3\left|H[\vec{k}]\right|\ , \tag{11}$$

---

[1] В предположении о равномерном распределении НЗБ в контейнере.
[2] Если для встраивания информации коэффициенты ДКП квантованы, то ошибка, введенная в этом процессе, является детерминированной функцией коэффициентов. Поскольку такая ошибка в данной структуре считалась бы стегошумом, сильная зависимость между коэффициентами контейнера и стегошума не допускала бы прямого анализа аддитивного шума.

где k – последовательность из восьмой части индексов, т.е. $k = [0,...,(N/2)-1]^3$.

Комбинируя величины из (11) можно получить точки 3-х мерного пространства для определения центра масс для ХФГ в случае RGB-пространства.

Для обнаружения наличия встроенной информации в принятом изображении в качестве детектора в [1] предложено использовать $C(H[k])$, значение которого сравнивается с наперед заданным порогом.

Авторы [1] провели тестовые эксперименты по обнаружению встроенной информации в цветном изображении. При этом ожидалось, что для 3-мерных гистограмм изображения RGB при встраивании дополнительной информации центр масс будет двигаться к началу координат.

Для проверки предположения о движении центра масс использовались 24 изображения, полученные на Kodak PhotoCD PCD0992. Это были 24-битовые изображения, размером 768x512 пикселей, сохраненные без потерь в формате PNG для 3-цветного изображения.

Для каждого из них вычислялся ЦМ ХФГ для оригинального изображения и для стегоизображения, полученного методом расширения спектра (МРС), при нормальном распределении шума $N(0,1)$ и 100% встраивании (т.е. $\alpha = 1$). На рис. 1 показан график разброса ЦМ ХФГ в 3-мерном пространстве (кружочки соответствуют оригинальным изображениям (Original), а крестики МРС стегоизображениям (SSIS)). Как ожидалось, ЦМ ХФГ стеганограмм находятся значительно ниже, чем ЦМ ХФГ оригиналов.

Применение предложенного метода обнаружения встроенной информации требует проведения процедуры выбора порога обнаружения.

Такой выбор возможен на основе наперед известных или каким-то образом оцененных статистических данных о ЦМ ХФГ (математическое ожидание и дисперсия).

Эта задача достаточно сложна, поскольку на выбор порога будет влиять выбор исходного множества изображений для оценки статистических данных.

Статистической мерой для выбора порога обнаружения в [1] было расстояние Махаланобиса.

Предполагалось, что распределение ЦМ ХФГ является Гауссовым. Был выбран учебный набор изображений для определения среднего значения μ и ковариации Σ матрицы исходных распределений, которые оценивались по формулам

$$\mu_i = \frac{1}{S}\sum_{k=0}^{S-1} x_i^{(k)}, \quad \Sigma_i = \frac{1}{S}(x_i - \mu_i)^T (x_i - \mu_i),$$

где x_i – учебный набор для i-го элемента, и S – число выборок. Для неизвестной схемы встраивания определялось расстояние Махаланобиса,

$$d^2 = (\vec{x} - \mu)^T \Sigma^{-1} (\vec{x} - \mu).$$

Расстояние Махаланобиса является статистической мерой того, как далеко находится данная точка от предполагаемого среднего для каждой переменной с учетом дисперсии. Вообще говоря, чем больше расстояние Махаланобиса, тем менее вероятно контрольной точке иметь такое же распределение, как в обучающем наборе. Поверхность, определенная уравнением $d^2 = 1$, является поверхностью, где каждая точка равна одному среднеквадратичному отклонению от среднего.

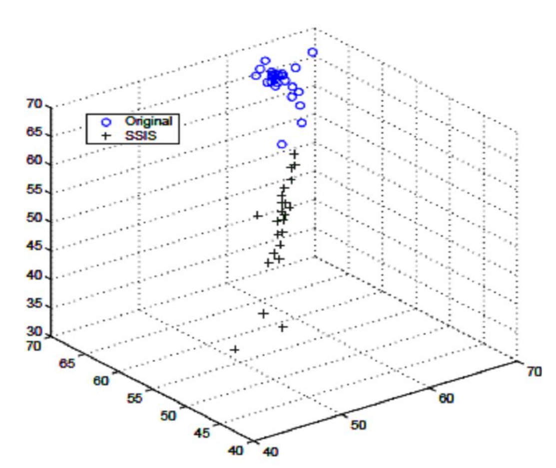


Рисунок 1 – Центры масс для тестовых изображений

Для проверки предложенной схемы 24 изображения случайным образом разделили на 5 групп:

1) для оценивания μ и Σ использовались ЦМ ХФГ от 20 оригинальных изображений;

2) классифицировался ЦМ от 1 неизменного изображения;

3) классифицировался ЦМ от 1 изображения МРС;

4) классифицировался ЦМ от 1 ДКП изображения;

5) классифицировался ЦМ от 1 НЗБ изображения.

Описанный многомерный случай рассматривался как естественное распределение ЦМ ХФГ, и любые значительно отличающиеся изображения классифицировались как содержащие стеганографические данные.

Расстояние Махаланобиса было выбрано на уровне 40, это обеспечивало норму ошибки первого типа (ложная тревога) около 5%. Норма правильной классификации оказалась около 95%.

2 Калибровочные датчики Керра

Кер [2] попытался использовать детектор Хармзена и Пеарлмена для обнаружения встроенной информации в полутоновых изображениях и пришел к выводу о его неэффективности в данном случае. Но, используя теорию Хармзена и Пеарлмена, Кер предложил два новых детектора на основе ЦМ ХФГ.

По мнению Кера, авторы [1] использовали очень ограниченный и гомогенный набор испытательных контейнеров, что привело к раздутым результатам эффективности их метода. Для полутоновых изображений метод должен был давать позитивное решение о наличии стего, если $C(H[k])$ превышает заданный порог. При проверке на практике оказалось, что в общем случае метод не срабатывает. Кер нашел причину и продемонстрировал свою догадку на примере 100 изображений от четырех разных источников (рис. 2).

На рис. 2 диаграмма разделена по источникам изображений. На диаграмме видно, что крестики почти все находятся ниже, чем соответствующие кружочки (метод в целом работает). Однако, значения ЦМ ХФГ сильно зависят от источника контейнеров, и среди $C(H_C[k])$ существует большой разброс. Часто разброс намного больше, чем типичные различия между $C(H_C[k])$ и $C(H_S[k])$. Существенная слабость детектора [1] в том, что он не знает $C(H_C[k])$.

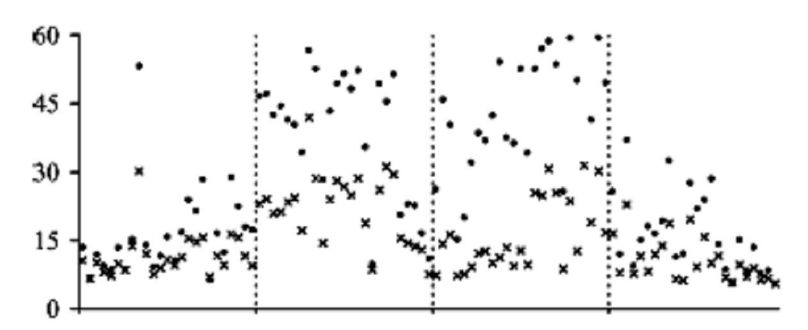


Рисунок 2 – Значения $C(H[k])$ *(кружочки)* до и *(крестики)* после встраивания

для 100 изображений от четырех различных источников

Кер объясняет различие в гистограммах цветных и полутоновых изображений следующим образом. В цветных изображениях, в основном, гистограммы довольно разрежены, с цветами, входящими в кластеры. Для пикселей в полутоновых изображениях существует всего N возможностей (в отличие от N^3*)*, поэтому там нет такой кластеризации. В результате появляется искажение ЦМ ХФГ, которое поглощает способность детектора отличать контейнеры от стеганограмм.

Свои детекторы Кер [2] создавал для обнаружения встроенной информации, когда для встраивания использовался метод соответствия НЗБ с нормой встраивания α. Он обосновал возможность применения теоремы 4 для этого случая. Пусть I_C – полутоновое изображение, I_S – стегоизображение, полученное из I_C. Соответственно, h_C и h_S – их гистограммы. Функция распределения масс аддитивного шума $f_\Delta[n]$ зависит от α, т.е. $f_\Delta[n] = f_\alpha$ и может принимать два значения

$$f_\alpha(0) = 1 - \alpha/2, \quad f_\alpha(1) = f_\alpha(-1) = \alpha/4.$$

Иными словами, 1 и -1 встраиваются с вероятностью $\alpha/4$, и с вероятностью $1-\alpha/2$ встраивание либо не производится, либо для встраивания ничего не нужно менять. С учетом встраивания методом соответствием НЗБ $h_S = f_\alpha * h_C$.

В области ДПФ,

$$H_S(k) = F_\alpha(k) H_C(k),$$

функцию f_α легко вычислить, она не равна нулю только в трех точках

$$F_\alpha(k) = \frac{\alpha}{4}\left(\cos(-\frac{2\pi k}{N}) - i\sin(-\frac{2\pi k}{N})\right) + \frac{\alpha}{4}\left(\cos(\frac{2\pi k}{N}) - i\sin(\frac{2\pi k}{N})\right) +$$

$$+ (1-\frac{\alpha}{2})\big(\cos(0) - i\sin(0)\big) =$$

$$= \frac{\alpha}{4}\left(\cos(\frac{2\pi k}{N}) + i\sin(\frac{2\pi k}{N})\right) + \frac{\alpha}{4}\left(\cos(\frac{2\pi k}{N}) - i\sin(\frac{2\pi k}{N})\right) + (1-\frac{\alpha}{2}) =$$

$$= 1 - \frac{\alpha}{2} + \frac{\alpha}{2}\cos(\frac{2\pi k}{N}) = 1 - \frac{\alpha}{2}\left(1 - \left(1 - \sin^2(\frac{\pi k}{N})\right)\right) = \left(1 - \alpha\sin^2(\frac{\pi k}{N})\right).$$

Соответственно для ХФГ стеганограммы получаем нужное неравенство

$$H_S(k) = F_\alpha(k) H_C(k) = (1 - \alpha\sin^2(k\pi/N))\tilde{h}_C(k) \le \tilde{h}_C(k). \quad (12)$$

Из (12) следует, что $C(I_S) \le C(I_C)$, т.е. после встраивания методом соответствия НЗБ величина ЦМ ХФГ не возрастает. Значит, можно воспользоваться теоремой 4.

Вместо пороговой оценки ЦМ ХФГ Кер [2] предложил использовать отношение ЦМ ХФГ гистограммы принятого изображения I к ЦМ ХФГ гистограммы гипотетического изображения $\bar{I}$. Пусть $\bar{I}$ – целочисленный выход усредняющего фильтра от принятого изображения I (т.е. $\bar{I}$ калиброванное изображение – downsampled image) с величинами пикселей[1]

$$\bar{I}_{i,j} = \left\lfloor \left(I_{2i,2j} + I_{2i+1,2j} + I_{2i,2j+1} + I_{2i+1,2j+1} \right) / 4 \right\rfloor. \qquad (13)$$

Кер высказал предположение, что процедура калибровки (13) будет менять контейнер незначительно, поскольку НЗБ соседних пикселей часто совпадают. В стеганограмме НЗБ совпадают значительно реже, поэтому калибровка вызовет более заметные изменения. Правильность этого предположения он подтвердил экспериментально (рис. 3). Более того, оказалось, что для большинства изображений экспериментально подтверждается (рис. 4) выполнение неравенства

$$C(H_C[k]) - C(H_S[k]) > C(H'_C[k]) - C(H'_S[k]) .$$

Во многих случаях, особенно когда норма встраивания близка к 100%, можно считать, что НЗБ в стеганограмме имеют равномерное распределение. Поэтому изображение $\bar{I}$ можно рассматривать как гипотетический контейнер.

Экспериментальные результаты [2] также подтвердили, что для большинства стеганограмм, созданных методом соответствия НЗБ, выполняется неравенство $C(I) < C(\bar{I})$. Детектор Кера $C(I)/C(\bar{I})$ является безразмерным детектором и был назван калибровочным детектором ЦМ ХФГ.

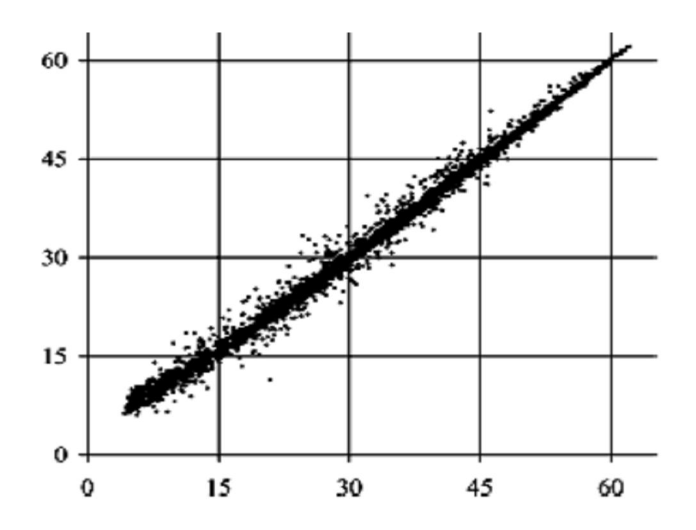


Рисунок 3 – График разброса для 2000 JPEG изображений
(ось X) ЦМ ХФГ калиброванных контейнеров, *(ось Y)* некалиброванных

[1] $\left\lfloor \frac{\cdot}{4} \right\rfloor$ означает деление нацело.

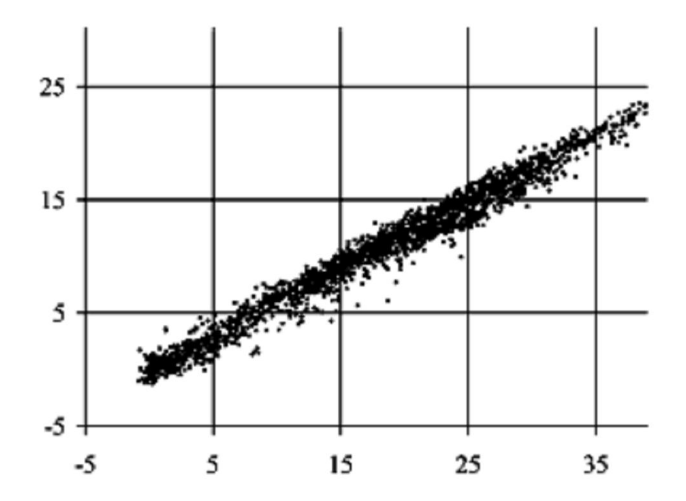


Рисунок 4 – График разброса для 2000 JPEG изображений: *(ось X)* $C(H_C[k]) - C(H_S[k])$ обычно больше, чем у калиброванных *(ось Y)* $C(H'_C[k]) - C(H'_S[k])$

Вторым детектором Кера [2] стал модифицированный детектор Харзмена и Пеарлмена. Кер искусственно приспособил его к полутоновым изображениям. Он попытался подправить основное различие между цветными и полутоновыми изображениями, обусловленное большей разреженностью гистограммы первого. Чтобы сделать гистограмму полутонового изображения более разреженной, Кер рассмотрел двумерную *гистограмму смежности.* Гистограмма смежности показывает, как часто по горизонтали для соседних пикселей наблюдается одинаковая интенсивность: $h_C^2(n) = \{(i,j) \big| p_C(i,j) = m, p_C(i,j+1) = n\}$. Поскольку смежные пиксели стремятся иметь близкие значения интенсивности, эта гистограмма разрежена по отношению к диагонали. Стеганография влияет на нее таким же образом, как на обычную гистограмму.

Используя двумерное ДПФ, Кер сформировал двумерную ХФГ $H^2[k]$ и двумерный ЦМ. Чтобы создать одномерный детектор, так или иначе необходимо было объединить двумерный ЦМ. Ввиду симметрии между двумя компонентами Кер использовал только один квадрант ДПФ и просто взял сумму компонентов

$$C^2(H^2[k,l]) = \frac{\sum_{i,j=0}^{n}(i+j)\left|H^2[i,j]\right|}{\sum_{i,j=0}^{n}\left|H^2[i,j]\right|}.$$

Ожидалось, что в присутствии стеганографии значение ЦМ будет меньшим. Так же, как в [1], этому детектору требовалось задавать порог обнаружения.

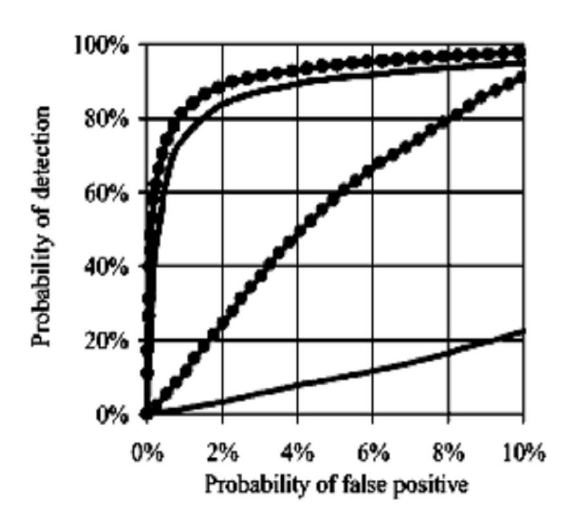
Для проверки работы своих датчиков Кер использовал два типа изображений.

1) 3000 распакованных изображений. Полная USDA NRCS. Фотогалерея http://фотогалерея. nrcs.usda.gov.

Изображения были загружены как TIF файлы с очень высоким разрешением (главным образом 2100x1500). Изначально они были отсканированы с множества пленок и бумажных источников. Для проверки изображения сжимались до размера 640x418 (для сжатия была выполнена перевыборка) и преобразовывались в полутоновые.

2) 20 000 JPEG изображений. Это были готовые фотографии с коэффициентом качества 58 (довольно сильно сжатые) и размерами приблизительно 640x400. Перед использованием фотографии преобразовались в полутоновые.

Экспериментирование показало, что в случае встраивания сообщений максимальной длины новые детекторы намного надежнее. На рис. 5 показаны графики вероятности правильного обнаружения (Probability of detection) от вероятности ложного обнаружения (Probability of false positive). К сожалению, Кер делает вывод, что обнаружение встроенной информации в распакованных контейнерах (которые еще до встраивания содержали много искажений) вполне возможно, но обнаружение встроенной информации в сжатых JPEG контейнерах становится надежным.



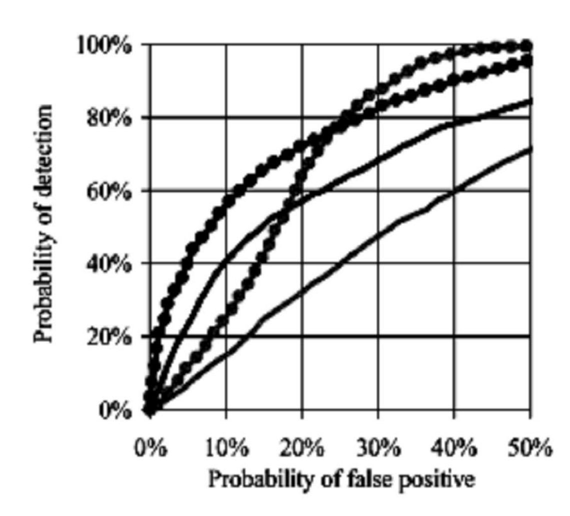


Рисунок 5 – Экспериментальные результаты для четырех видов детекторов: две серые линии для детекторов ЦМ ХФГ (сплошная для полномасштабных изображений и точечная для калиброванных), две черные линии для детекторов ЦМ ХФГ на гистограмме смежности (сплошная для полномасштабного изображений и точечная для калиброванного)

Кроме того, по результатам проведенных экспериментов Кера, представленная методика калибровки работает плохо, если количество скрытых данных меньше максимально возможного. Использование гистограммы смежности все еще улучшает ситуацию, но калибровка уже не приносит существенной выгоды. Причину Кер видит в том, что при встраивании более коротких сообщений ЦМ ХФГ калиброванного стего и ЦМ ХФГ пустого контейнера уменьшаются не существенно. Проблема остается нерешенной.

3 Калибровочные датчики Ли

Хаолонг Ли и его команда [3] предложили модифицировать датчики Кера, отказавшись использовать центр масс ХФГ. Они использовали функцию отношений модуля ХФГ принятого изображения к модулю ХФГ калиброванного изображения. Пусть для изображения I

$$d(k,I)=|H(k)|/|H'(k)| \quad , \qquad (14)$$

где H' есть ДПФ h' – гистограммы калиброванного изображения $\bar{I}$. Предполагалось[1], что поскольку изображение $\bar{I}$ является «сглаженной» версией изображения I,

[1]Правильность первой теоремы в [3] (приведенной без доказательства) вызывает сомнения, теоретическое обоснование правомочности выбора $d(k,I)$, как и все дальнейшие исследования, основывались на этой теореме.

то для принятого контейнера будет выполняться соотношение $d(k,\bar{I}_C) \approx d(k,\bar{I})$ и для принятого стего $d(k,\bar{I}_S) \le d(k,\bar{I})$, аналогичные соотношениям $C(I) \approx C(\bar{I})$ и $C(I) < C(\bar{I})$ в [2]. Соответственно предполагалось, что отношение $d(k,I)$ уменьшается после встраивания соответствием НЗБ (так же как $C(I)$). Ожидалось, что в высокочастотной области (для больших *k*) $d(k,I)$ будет сильно осциллировать, поэтому минимальное значение $d(k,I)$, рассчитанное по формуле (14), было ограничено единицей, т.е. рассматривалось «отклоненное» $d(k,I)$

$$d_*(k,I_S) = \min\{d(k,I),1\}.$$

Как детектор использовалась величина:

$$D_1(I) = \frac{\sum_{k=0}^{N/2} s_k d_*(k,I)}{\sum_{k=0}^{N/2} s_k}, \quad (15)$$

где $s_k \ge 0$ – весовые коэффициенты. Из неравенства $d(k,\bar{I}_S) \le d(k,\bar{I})$ непосредственно следует $D_1(I_S) \le D_1(I_C)$.

Следующее предположение Ли и его коллег состояло в том, что при калибровке пиксели с меньшим колебанием будут меньше изменять гистограмму контейнера, и производительность обнаружения улучшится. Поэтому в [3] было предложено уменьшить размер изображения, оставляя только «гладкие» пиксели. Для каждого набора из четырех соседних пикселей

$$S_{i,j} = \{2i+i', 2j+j'\} \in I_C : i', j' \in \{0,1\}$$

определялась характеристика колебания $D_{i,j}$

$$D_{i,j} = \left|I_{2i,2j} - I_{2i,2j+1}\right| + \left|I_{2i,2j+1} - I_{2i+1,2j+1}\right| + \left|I_{2i+1,2j+1} - I_{2i+1,2j}\right| + \left|I_{2i+1,2j} - I_{2i,2j}\right|.$$

Далее для заданного порога *T* определялась подпоследовательность

$$ps(I) = \{S_{i,j} : D_{i,j} < T\},$$

которая рассматривалась как уменьшенное изображение. Окончательно детектор задавался равенством $D^{ps}{}_1(I) = D_1(ps(I))$. Точнее, последовательно выполняются три шага: для определенного порога *T* выбирается «гладкое» изображение $ps(I)$; выполняется калибровка $ps(I)$; по формуле (14) вычисляется $d(k, ps(I))$ (изображение I заменено $ps(I)$); и, наконец, по формуле (15) получается детектор $D_1(ps(I))$. Это был первый вариант калибровочных детекторов Ли.

Но авторы [3] не остановились на этом и предложили еще одну модификацию детектора. Они предложили заменить исходное изображение на «отличающее» изображение I^d, которое определяли через разницу величин смежных пикселей полутонового изображения I:

$$I^d_{i,j} = I_{2i,j} - I_{2i+1,j} + 255. \quad (16)$$

Значения пикселей в I^d меняются от 0 до 510. Идея состоит в том, что «отличающее» изображение I^d лучше покажет наличие искажения от встраивания (по

сравнению с оригинальным изображением I). Скорее всего, распределение значений пикселей I^d будет сконцентрированным. После встраивания сообщения для оригинального изображения максимальные изменения величин пикселей равны 1, а для «отличающего» изображения максимальные изменения величин пикселей равны 2.

В [3] приводятся экспериментальные результаты сравнения работы 3-х типов детекторов на 3000 изображений: детектора для «отличающего» изображения $C(I^d)/C(\bar{I}^d)$; детектора для оригинального изображения $C(I)/C(\bar{I})$; и детектора $C(I^s)/C(\bar{I}^s)$ для суммарного изображения I^S, определенного как $I^I_{i,j} = I_{2i,j} + I_{2i+1,j}$.

На рис. 6 показаны графики вероятности обнаружения встроенной информации (Probability of detection) от вероятности ложного обнаружения (Probability of false positive) для трех типов калибровочных датчиков, основанных на трех типах изображений («отличающего» $C(I^d)/C(\bar{I}^d)$, суммарного $C(I^s)/C(\bar{I}^s)$ и оригинального $C(I)/C(\bar{I})$).

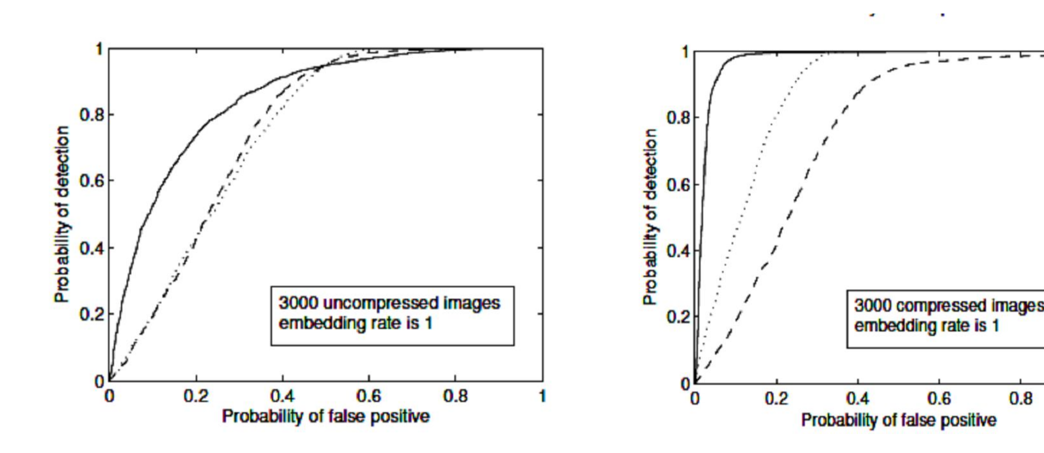


Рисунок 6 – Экспериментальные результаты для трех видов датчиков: «отличающих» (сплошная), суммарного (точечная) и оригинального изображение - (штриховая), соответственно

Приведенные экспериментальные результаты подтверждают целесообразность применения процедуры выбора сглаженного изображения и последующего его сжатия. Из графиков на рис. 6 ясно видно, что детектор на «отличающем» изображении работает намного лучше двух других.

Заключение

Теория, созданная Хармзеном и Пеарлменом [1], стала основой для развития нового направления в статистическом стеганоанализе. Создание безразмерного калибровочного детектора Керра [2], который не требует проведения сложной процедуры предварительного определения порога обнаружения, было существенным шагом в развитии этого направления. Кроме того, Кер экспериментально доказал право на применение калибровки к принятому изображению для получения оценки пустого контейнера. Важным шагом в работе Ли и его команды [3] следует считать использование уменьшенного сглаженного и «отличающего» изображений. К сожалению, в работе нет информации о зависимости вероятности обнаружения от нормы встраивания α.

Судя по всему, авторы использовали максимальное наполнение контейнера. Возможно, использование калибровочного детектора Кера на гистограмме смежности дало бы результат, схожий с результатами для детектора на «отличающем» изображении. Это пока открытый вопрос.

Литература

1. Jeremiah J. Harmsen and William A. Pearlman. Steganalysis of additive noise modelable information hiding / J. Jeremiah // Proc. SPIE. – 2003. – № 5022. – P. 131-142.
2. Andrew D. Ker, Steganalysis of LSB Matching in Grayscale Images / D. Andrew // IEEE Signal Processing Letters. – June 2005. – VOL. 12, № 6. – P. 441-444
3. Li X. Detecting LSB Matching by Applying Calibration Technique for Difference Image / X. Li, T. Zeng, B. Yang // Proc. 10th ACM Workshop on Multimedia and Security. – Oxford, U.K., 2008. – P. 133-138.
4. Niels Provos. Hide and Seek: Introduction to Steganography / Niels Provos, Peter Honeyman // IEEE security and Privacy. – May 2003. – Vol. 1, Issue 3. – Pages: 32-44.

RESUME

L.L. Nikitenko

Methods Based on Steganalysis Calibration Technology Programs

Work is devoted the review of statistical steganoanalysis methods of digital images, that created on the basis of estimation of centre-of-mass of discrete Fourier transformation of image histograms. Theoretical bases for creation of technology of the examined methods are developed in supposition about additive hiding of additional information. The first detectors are requiring the difficult selection procedure of detection threshold. The threshold value is depending on a teaching sequence that is limiting an application domain of methods. Application of the calibration procedure to the accepted image allowed estimating the hypothetical container histogram and creating the dimensionless detectors of the hiding information. An exception from the accepted image the «unsmooth» areas allowing outperform of detection. Effect of additive distortion on signal statistics was analyzed for the hiding norm $\alpha \le 100\%$.

Статья поступила в редакцию 09.04.2013.